No. 17-2

In the Supreme Court of the United States

UNITED STATES OF AMERICA, PETITIONER

v.

MICROSOFT CORPORATION

ON WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

BRIEF FOR THE UNITED STATES

NOEL J. FRANCISCO
Solicitor General
Counsel of Record
JOHN P. CRONAN
Acting Assistant Attorney General
MICHAEL R. DREEBEN
Deputy Solicitor General
MORGAN L. GOODSPEED
Assistant to the Solicitor General
ROSS B. GOLDMAN
Attorney

Department of Justice
Washington, D.C. 20530-0001
SupremeCtBriefs@usdoj.gov
(202) 514-2217

QUESTION PRESENTED

Whether a United States provider of email services must comply with a probable-cause-based warrant issued under 18 U.S.C. 2703 by making disclosure in the United States of electronic communications within that provider's control, even if the provider has decided to store that material abroad.

TABLE OF CONTENTS

Page

Opinions below 1
Jurisdiction 1
Statutory provisions involved 2
Statement 2
Summary of argument 12
Argument:
Under 18 U.S.C. 2703, the government may require a U.S. service provider to disclose any electronic communicatons within its control 16
A. This case involves a domestic application of Section 2703 18
1. This Court's decisions require a provision-specific "focus" analysis 18
2. Section 2703 focuses on the disclosure of electronic communications in the United States ... 21
3. Even if Section 2703 focuses on privacy, any invasion of privacy occurs in the United States 26
B. Congress enacted Section 2703 against the background principle that subpoena recipients must produce all records within their control 32
C. Microsoft's contrary theory would be both impractical and detrimental to law enforcement 41
D. Enforcement of Section 2703 respects the United States' international obligations 46
Conclusion 53
Appendix — Statutory provisions 1a

TABLE OF AUTHORITIES

Cases:

Birchfield v. *North Dakota*, 136 S. Ct. 2160 (2016) 28
Braswell v. *United States*, 487 U.S. 99 (1988) 33
California v. *Hodari D.*, 499 U.S. 621 (1991) 30

Cases—Continued: Page

California Bankers Assn. v. *Shultz*, 416 U.S. 21 (1974) 30
City of L.A. v. *Patel*, 135 S. Ct. 2443 (2015) 38
Donovan v. *Lone Steer, Inc.*, 464 U.S. 408 (1984) .. 30, 35, 38
EEOC v. *Arabian Am. Oil Co.*, 499 U.S. 244 (1991) 46
Fisher v. *United States*, 425 U.S. 391 (1976) 41
Gambino v. *United States*, 275 U.S. 310 (1927) 29
Grand Jury Subpoena Served Upon Horowitz, In re, 482 F.2d 72 (2d Cir.), cert. denied, 414 U.S. 867 (1973) 40
Grand Jury Subpoenas Dated March 19, 2002 and August 2, 2002, In re, 318 F.3d 379 (2d Cir. 2003) 45
Hay Grp., Inc. v. *E.B.S. Acquisition Corp.*, 360 F.3d 404 (3d Cir. 2004) 32
Information Associated with One Yahoo Email Address That Is Stored at Premises Controlled by Yahoo, In re, No. 17-M-1234, 2017 WL 706307, (E.D. Wis. Feb. 21, 2017) 22
Kastigar v. *United States*, 406 U.S. 441 (1972) 30
Kiobel v. *Royal Dutch Petroleum Co.*, 569 U.S. 108 (2013) 46
Kirtsaeng v. *John Wiley & Sons, Inc.*, 568 U.S. 519 (2013) 32
Linde v. *Arab Bank, PLC*, 706 F.3d 92 (2d Cir. 2013), cert. denied, 134 S. Ct. 2869 (2014) 51
Liu Meng-Lin v. *Siemens AG*, 763 F.3d 175 (2d Cir. 2014) 20
Loginovskaya v. *Batratchenko*, 764 F.3d 266 (2d Cir. 2014) 20
Los Angeles Cnty. v. *Rettele*, 550 U.S. 609 (2007) 35
Maracich v. *Spears*, 133 S. Ct. 2191 (2013) 41

Cases—Continued: Page

Marc Rich & Co. v. *United States*, 707 F.2d 663 (2d Cir.), cert. denied, 463 U.S. 1215 (1983) 7, 14, 33
Microsoft Corp. v. *AT&T Corp.*, 550 U.S. 437 (2007) 17
Morrison v. *National Austl. Bank Ltd.*, 561 U.S. 247 (2010) 13, 17, 18, 19, 20, 23
Oklahoma Press Publ'g Co. v. *Walling*, 327 U.S. 186 (1946) 38
RJR Nabisco, Inc. v. *European Cmty.*, 136 S. Ct. 2090 (2016) ..... *passim*
Reinsurance Co. of Am., Inc. v. *Administratia Asigurarilor de Stat*, 902 F.2d 1275 (7th Cir. 1990) 51
Sealed Case, In re, 832 F.2d 1268 (D.C. Cir. 1987) 33, 51
Search of Information Associated with Accounts Identified as [redacted]@gmail.com, In re, No. 16-mj-2197, 2017 WL 3263351 (C.D. Cal. July 13, 2017) 21
Search of Information Associated with [Redacted]@gmail.com That is Stored at Premises Controlled by Google, Inc., In re, No. 16-mj-757, 2017 WL 3445634, (July 31, 2017), aff'g 2017 WL 2480752 (D.D.C. June 2, 2017) 21, 43, 45
Search of Premises Located at [Redacted]@yahoo.com, In re, No. 17-mj-1238 (M.D. Fla. Apr. 7, 2017) 22
Search Warrant Issued to Google, Inc., In re, No. 17-mj-532, 2017 WL 4022806 (N.D. Ala. Sept. 1, 2017) 21
Search Warrant No. 16-960-M-1 to Google, In re:
232 F. Supp. 3d 708 (E.D. Pa. 2017) 45
No. 16-960, 2017 WL 3535037 (Aug. 17, 2017), aff'g 232 F. Supp. 3d 708 (E.D. Pa. 2017) 21
Search Warrant to Google, Inc., In re, No. 16-4116, 2017 WL 2985391, (D.N.J. July 10, 2017) 22

Cases—Continued: Page

Securities and Exchange Comm'n v. *Minas de Artemisa*, 150 F.2d 215 (9th Cir. 1945) 34
Skinner v. *Railway Labor Execs.' Ass'n*, 489 U.S. 602 (1989) 29
Societe Internationale pour Participations Industrielles et Commerciales, S. A. v. *Rogers*, 357 U.S. 197 (1958) 52
Société Nationale Industrielle Aérospatiale v. *United States Dist. Court*, 482 U.S. 522 (1987) 34, 51
Soldal v. *Cook Cnty.*, 506 U.S. 56 (1992) 30, 31
Superintendent of Ins. of N.Y. v. *Bankers Life & Cas. Co.*, 404 U.S. 6 (1971) 18, 23
The Matter of the Search of Information Associated with [REDACTED]@gmail.com that is stored at premises controlled by Google, In re, No. 17-7131 (D. Ariz. Aug. 21, 2017) 21
The Search of Content Stored at Premises Controlled by Google Inc., In re:
No. 16-mc-80263, 2017 WL 1487625 (N.D. Cal. Apr. 25, 2017) 43
No. 16-mc-80263, 2017 WL 3478809 (Aug. 14, 2017), aff'g 2017 WL 1487625 (N.D. Cal. Apr. 25, 2017) 21
TianRui Grp. v. *Int'l Trade Comm'n*, 661 F.3d 1322 (Fed. Cir. 2011) 20
Two Email Accounts Stored at Google, Inc., In re, No. 17-M-1235, 2017 WL 2838156 (E.D. Wis. June 30, 2017) 22
United States v. *All Assets Held at Bank Julius*, 251 F. Supp. 3d 82 (D.D.C. 2017) 20
United States v. *Ballestas*, 795 F.3d 138 (D.C. Cir. 2015), cert. denied, 136 S. Ct. 1229 (2016) 20

Cases—Continued: Page

United States v. *Bank of Nova Scotia*, 740 F.2d 817 (11th Cir. 1984), cert. denied, 469 U.S. 1106 (1985) 33
United States v. *Barr*, 605 F. Supp. 114 (S.D.N.Y. 1985) 41
United States v. *First Nat'l City Bank*, 396 F.2d 897 (2d Cir. 1968) 33, 34
United States v. *Google, Inc.*, No. 17-mc-7 (W.D. Tenn. Nov. 3, 2017) 21
United States v. *Grubbs*, 547 U.S. 90 (2006) 38
United States v. *Hubbell*, 530 U.S. 27 (2000) 30
United States v. *Jacobsen*, 466 U.S. 109 (1984) 30, 31
Yates v. *United States*, 135 S. Ct. 1074 (2015) 22
Zurcher v. *Stanford Daily*, 436 U.S. 547 (1978) 35

Constitution, treaty, statutes, and rules:

U.S. Const.:
Amend. IV 4, 9, 30
Amend. V 30
Council of Europe Convention on Cybercrime, Nov. 23, 2001, S. Treaty Doc. No. 11, 108th Cong., 1st Sess. (2003), 2296 U.N.T.S. 167 48
Preamble 48
Arts. 16-21 49
Art. 18 49
Art. 18.1(a) 48
Explanatory Report (Nov. 8, 2001) 48, 49
Letter of Transmittal (Nov. 17, 2003) 49
Letter of Submittal (Sept. 11, 2003) 48
Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (18 U.S.C. 2510 *et seq.*) 2
18 U.S.C. 2510(15) 2

Statutes and rules—Continued: Page

Racketeer Influenced and Corrupt Organization Act, 18 U.S.C. 1961 *et seq.* 18
18 U.S.C. 1962 ..... 18, 19
18 U.S.C. 1962(a) 18
18 U.S.C. 1962(b) 18
18 U.S.C. 1962(c) 18
18 U.S.C. 1962(d) 18
18 U.S.C. 1964 ..... 18, 19
Securities Exchange Act of 1934, 15 U.S.C. 78a *et seq.*:
15 U.S.C. 78j(b) (§ 10(b)) 19
15 U.S.C. 78dd(a) (§ 30(a)) 20
Stored Communications Act, Pub. L. No. 99-508, Tit. II, 100 Stat. 1860 (18 U.S.C. 2701 *et seq.*):
18 U.S.C. 2701 ..... 8, 20, 1a
18 U.S.C. 2701-2712 2
18 U.S.C. 2701(a) 27, 1a
18 U.S.C. 2701(c)(1) 27, 2a
18 U.S.C. 2702 ..... 8, 27, 28, 2a
18 U.S.C. 2702(a) 27, 2a
18 U.S.C. 2702(a)(1) 28, 2a
18 U.S.C. 2702(b)(2) 28, 4a
18 U.S.C. 2702(b)(4)-(5) 27, 4a
18 U.S.C. 2702(c)(1) 28, 5a
18 U.S.C. 2702(c)(3) 27, 5a
18 U.S.C. 2703 (§ 201, 100 Stat. 1861) ..... *passim*, 6a
18 U.S.C. 2703(a) ..... *passim*, 6a
18 U.S.C. 2703(a)-(c) 23, 28, 6a, 7a, 8a
18 U.S.C. 2703(b) 4, 13, 15, 22, 7a
18 U.S.C. 2703(b)(1) 16, 35, 7a
18 U.S.C. 2703(b)(1)(A) 4, 34, 36, 39, 7a

Statutes and rules—Continued: Page

18 U.S.C. 2703(b)(1)(B) 3, 7a
18 U.S.C. 2703(b)(1)(B)(i) 3, 40, 7a
18 U.S.C. 2703(b)(1)(B)(ii) 3, 7a
18 U.S.C. 2703(c) 13, 15, 22, 8a
18 U.S.C. 2703(c)(1) 3, 35, 8a
18 U.S.C. 2703(c)(1)(A) 4, 16, 36, 39, 8a
18 U.S.C. 2703(c)(2) 3, 9a
18 U.S.C. 2703(d) 3, 4, 22, 38, 10a
18 U.S.C. 2703(e) 23, 10a
18 U.S.C. 2703(f) 23, 11a
18 U.S.C. 2703(g) 23, 36, 37, 11a
18 U.S.C. 2705(a) 3
18 U.S.C. 2707 8
18 U.S.C. 2711(2) 2, 12a
18 U.S.C. 2711(3)(A) 37, 12a
Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Tit. II, Pub. L. No. 107-56, 115 Stat. 272 (18 U.S.C. 1 *et seq.*):
§ 212, 115 Stat. 284 24
§ 212, 115 Stat. 284-285 ..... 13, 22
§ 212(b), 115 Stat. 285 24
§ 220(a)(1), 115 Stat. 291-292 37
18 U.S.C. 3105 35
Fed. R. Crim. P.:
Rule 17(c)(1) 36
Rule 17(c)(2) 38
Rule 17(g) 38
Rule 41 ..... 35, 37
Rule 41(b)(1) 37

Rules—Continued: Page

Rule 41(d) 4
Rule 41(e)(1) 35
Rule 41(f)(1)(B) 35
Rule 41(f)(1)(C) 38

Miscellaneous:

ALI, *The Foreign Relations Law of the United States, Status Details*, https://www.ali.org/projects/show/foreign-relations-law-united-states/ (Dec. 6, 2017) 52

Cybercrime Convention Committee, Council of Europe, https://www/coe.int/en/web/cybercrime/guidance-notes, *T-CY Guidance Note #10* (Mar. 1, 2017) 48, 49

H.R. Rep. No. 647, 99th Cong., 2d Sess. (1986) 24

Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208 (2004) 4

Winston Maxwell & Christopher Wolf, *A Global Reality: Governmental Access to Data in the Cloud* (July 18, 2012), https://www.hldataprotection.com/uploads/file/Revised%20Government%20Access%20to%20Cloud%20Data%20Paper%20(18%20July%2012).pdf 47

Restatement (Fourth) of the Foreign Relations Law of the United States, Reporters' Note (2016) 52

Restatement (Third) of the Foreign Relations Law of the United States (1987) 51, 52

S. Exec. Rep. No. 6, 109th Cong., 1st Sess. (2005) 49

S. Rep. No. 541, 99th Cong., 2d Sess. (1986) 24

Miscellaneous—Continued: Page

Statement of Brad Wiegmann, Deputy Assistant Att'y Gen., DOJ, Before the Subcomm. On Crime & Terrorism, U.S. Senate Comm. on the Judiciary, Hearing entitled: *Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights* (May 24, 2017), https://www.judiciary.senate.gov/imo/media/doc/05-24-17%20Wiegmann%20Testimony.pdf 44, 45, 46, 50

9A Charles Alan Wright & Arthur R. Miller, *Federal Practice and Procedure* (3d ed. 2008) 32

In the Supreme Court of the United States

No. 17-2

UNITED STATES OF AMERICA, PETITIONER

v.

MICROSOFT CORPORATION

ON WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

BRIEF FOR THE UNITED STATES

OPINIONS BELOW

The opinion of the court of appeals (Pet. App. 1a-72a) is reported at 829 F.3d 197. The order denying rehearing en banc and the opinions concurring in and dissenting from that denial (Pet. App. 105a-154a) are reported at 855 F.3d 53. The orders of the district court (Pet. App. 99a-104a) are unreported. The opinion of the magistrate judge (Pet. App. 73a-98a) is reported at 15 F. Supp. 3d 466.

JURISDICTION

The judgment of the court of appeals was entered on July 14, 2016. A timely petition for rehearing was denied on January 24, 2017 (Pet. App. 105a-154a). On April 12, 2017, Justice Ginsburg extended the time within which to file a petition for a writ of certiorari to and including May 24, 2017. On May 15, 2017, Justice Ginsburg further extended the time to June 23, 2017,

and the petition was filed on that date. The jurisdiction of this Court rests on 28 U.S.C. 1254(1).

STATUTORY PROVISIONS INVOLVED

The relevant statutory provisions are reprinted in an appendix to this brief. App., *infra*, 1a-12a.

STATEMENT

1. In 1986, Congress enacted the Electronic Communications Privacy Act of 1986 (ECPA), Pub. L. No. 99-508, 100 Stat. 1848 (18 U.S.C. 2510 *et seq.*), to regulate government access to wire and electronic communications. Title II of that Act is often called the Stored Communications Act (SCA). See 18 U.S.C. 2701-2712; see also Pet. App. 12a. The SCA governs how stored wire and electronic communications may and may not be lawfully accessed and disclosed by an "electronic communications service" and a "remote computing service." See 18 U.S.C. 2701-2712.[1]

The SCA authorizes the government to require a provider of an electronic communication service or remote computing service to disclose information to the government about wire or electronic communications, including emails. See 18 U.S.C. 2703. Section 2703, captioned "Required disclosure of customer communications or records," provides three separate mechanisms for the government to acquire such information. *Ibid.*

First, the government may issue an "administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena."

---

[1] An "electronic communication service" "provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. 2510(15). A "remote computing service" provides "computer storage or processing services by means of an electronic communications system." 18 U.S.C. 2711(2).

18 U.S.C. 2703(b)(1)(B)(i). With a subpoena, the government may acquire basic subscriber information such as the subscriber's name and identifying information. 18 U.S.C. 2703(c)(2). A subpoena may also be used for the contents of emails stored by an electronic communication service for more than 180 days, 18 U.S.C. 2703(a) and (b)(1)(B)(i), and the contents of all emails stored by a remote computing service, 18 U.S.C. 2703(b)(1)(B)(i), if the government provides prior notice to the subscriber or complies with procedures that allow notice to be delayed by up to 90 days, 18 U.S.C. 2703(b)(1)(B), 2705(a).

Second, the government may obtain a court order, sometimes called a 2703(d) order, requiring disclosure of any of the records covered by a subpoena. 18 U.S.C. 2703(b)(1)(B)(ii). The same notice requirement applies to email content. 18 U.S.C. 2703(b)(1)(B). Under a 2703(d) order, the government may also acquire certain "other information pertaining to a subscriber," beyond basic account information and the contents of emails. 18 U.S.C. 2703(c)(1). The government may obtain a 2703(d) order only if it "offers specific and articulable facts showing that there are reasonable grounds to believe that" the records sought are "relevant and material to an ongoing criminal investigation." 18 U.S.C. 2703(d).

This case involves the third mechanism. The SCA authorizes the government to "require the disclosure" by a service provider of electronic communications and other records by means of a "warrant issued using the procedures described in the Federal Rules of Criminal Procedure * * * by a court of competent jurisdiction." 18 U.S.C. 2703(a) (covering electronic communication

services); see 18 U.S.C. 2703(b) (remote computing services); 18 U.S.C. 2703(c)(1)(A) (subscriber information). Under a Section 2703 warrant, the government may demand any of the same records covered by a 2703(d) order—without providing prior notice to a subscriber. 18 U.S.C. 2703(b)(1)(A). In addition, unlike with subpoenas and 2703(d) orders, the government may obtain the contents of communications stored by an electronic communication service for fewer than 181 days. 18 U.S.C. 2703(a). To do so, the government must satisfy a neutral judicial officer that there is probable cause to believe that the records to be disclosed contain evidence of a crime, and must describe those records with particularity. Fed. R. Crim. P. 41(d); see U.S. Const. Amend. IV.

As one commenter has observed, Section 2703's rules for compelled disclosure "operate like an upside-down pyramid." Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1222 (2004). A subpoena sits at the bottom of the hierarchy, subject to traditional relevance constraints but no particular statutory standard; a 2703(d) order comes next and requires specific and articulable facts showing that the requested materials are relevant to a criminal investigation; and a Section 2703 warrant sits at the top and requires a showing of probable cause. Consistent with the increasing demands on the government to show the relevance and significance of the requested materials, "[t]he higher up the pyramid you go, the more information the government can obtain." *Ibid.*

2. a. Microsoft is a United States corporation, incorporated and headquartered in Washington. Pet. App. 5a. It operates web-based email services such as

MSN, Hotmail, and Outlook. *Id.* at 5a & n.1. Microsoft stores the contents of users' emails—along with various other information associated with users' email accounts, such as IP addresses and lists of contacts—on a network of approximately one million servers. *Id.* at 6a-7a. Those servers are housed in approximately 100 datacenters located in 40 countries. *Id.* at 7a.

When a user signs up for a Microsoft email service, he is asked to identify where he is "from." J.A. 30; see Pet. App. 6a. The user then selects a country from a drop-down menu. J.A. 30-31. Microsoft does not verify his location. See Pet. App. 7a. Rather, Microsoft runs an automatic scan on newly created accounts and then "migrate[s]" the account data to a datacenter near the user's reported location. J.A. 31; see Pet. App. 7a. It does so in an effort to reduce "network latency," *i.e.*, the slower service that results from greater geographic distances between the datacenter and the user. J.A. 31.

One of Microsoft's datacenters is located in Dublin, Ireland. See Pet. App. 7a. When Microsoft migrates email content and other account information from the United States to the Dublin datacenter, the company deletes the content and much of the other information associated with the account from its domestic servers (while keeping several copies of the content in other places outside the United States for "redundancy"). J.A. 31; see Pet. App. 7a. Three "data sets" remain in the United States after the deletion: "some non-content email information"; "some information about the user's online address book"; and "some basic account information, including the user's name and country," as reported by the user. Pet. App. 7a-8a; see J.A. 31-32. Through a "database management program," however,

Microsoft's Global Criminal Compliance team can access account information stored anywhere in Microsoft's global network from its offices within the United States. Pet. App. 8a; J.A. 33-34.

b. In December 2013, the government applied for a Section 2703 warrant requiring Microsoft to disclose email information for a particular email account. Pet. App. 2a, 8a-10a. The government's application established probable cause to believe that the account was being used to further illegal drug activity in, or drug manufacturing for importation into, the United States. *Id.* at 2a; see J.A. 25 (listing potential violations of U.S. law).

A federal magistrate judge issued the requested Section 2703 warrant, concluding that the government had established probable cause to believe that the specified email account contained fruits, evidence, or instrumentalities of narcotics trafficking. See Pet. App. 2a; J.A. 25. The warrant covered "information associated with" an MSN.com email account "stored at premises owned, maintained, controlled, or operated by Microsoft Corporation." Pet. App. 9a (citation omitted). The warrant required Microsoft to "disclose * * * to the Government" the contents of emails stored in the account; some additional records "regarding the identification of the account," including the name and IP addresses associated with the account and the user's contact list; and "records pertaining to communications" between Microsoft and "any person" about the account. J.A. 24-25.

The government served Microsoft with the warrant at its headquarters in Redmond, Washington. Pet. App. 2a. In response, Microsoft disclosed certain account-identification records, which it stored in the United States. *Id.* at 10a. But Microsoft refused to disclose the

contents of the emails in the account, which it had "migrat[ed]" to its datacenter in Ireland. *Id.* at 7a, 10a. Microsoft then moved to quash the warrant as to all material stored abroad, arguing, *inter alia*, that it would be an impermissible extraterritorial application of Section 2703 to require a provider to disclose electronic information stored outside this country. See *id.* at 20a-21a, 73a-74a.

The magistrate judge denied the motion to quash. He explained that, although a Section 2703 warrant is "obtained" like a "conventional warrant" on a showing of probable cause, "it is executed like a subpoena." Pet. App. 84a. That is because "it is served on the [provider] in possession of the information and does not involve government agents entering the premises of the [provider] to search its servers and seize the e-mail account in question." *Ibid.* The magistrate judge concluded that Section 2703 does not "alter the basic principle"—which has "long been the law" with respect to subpoenas—that "an entity lawfully obligated to produce information" in its control "must do so regardless of the location of that information." *Id.* at 84a-85a (citing *Marc Rich & Co.* v. *United States*, 707 F.2d 663, 667 (2d Cir.), cert. denied, 463 U.S. 1215 (1983)).

On de novo review, the district court affirmed the magistrate judge's ruling. Pet. App. 102a. To facilitate appellate jurisdiction, the parties jointly stipulated that Microsoft had not complied with the warrant and did not intend to comply while it sought further review. J.A. 27-28. Given that stipulation, the court held Microsoft in civil contempt, though it did not impose any sanctions while Microsoft appealed. Pet. App. 103a.

3. a. A panel of the court of appeals reversed the denial of the motion to quash and vacated the civil contempt finding. Pet. App. 1a-48a. The panel ruled that enforcing the warrant as to information stored abroad would constitute an impermissible extraterritorial application of the statute. *Id.* at 47a.

The panel devoted a significant portion of its analysis to explaining that Section 2703's warrant provision does not apply extraterritorially. See Pet. App. 22a-36a. It then considered "the 'focus' of the relevant statutory provision," *id.* at 36a (citation omitted), to determine whether "conduct relevant to the statute's focus occurred in the United States," in which case the warrant "involves a permissible domestic application" of the statute "even if other conduct occurred abroad," *RJR Nabisco, Inc.* v. *European Cmty.*, 136 S. Ct. 2090, 2101 (2016). In the panel's view, "the SCA's focus lies primarily on the need to protect users' privacy interests." Pet. App. 39a. The panel grounded that conclusion in Section 2703's "appear[ance] in a statute entitled the Electronic Communications Privacy Act"; Section 2703's reference to the rules for issuance of warrants in the Federal Rules of Criminal Procedure; a reading of Sections 2701, 2702, and 2707 of the SCA, which it believed relate to privacy; and legislative history showing that the protection of privacy was a goal of the SCA. *Id.* at 37a-43a.

Next, the panel reasoned that "the invasion of the customer's privacy takes place under the SCA where the customer's protected content" is stored—here, in the Dublin datacenter. Pet. App. 43a. The panel asserted that a warrant requiring a provider to access a datacenter abroad calls for the provider to "seize[]" the data from that location while "acting as an agent of the

government." *Id.* at 43a-44a. And it concluded that the location of the provider's "seiz[ure]" was more relevant than the customer's actual location, Microsoft's home in the United States, or the location of U.S. law enforcement personnel. See *ibid.* Thus, the panel concluded that the conduct relevant to the statute's focus occurred outside the United States. *Id.* at 47a.

b. Judge Lynch concurred in the judgment, describing "the sole issue" in the case as "whether Microsoft can thwart the government's otherwise justified demand for the emails at issue by the simple expedient of choosing—in its own discretion—to store them on a server in another country." Pet. App. 52a. He disagreed with the notion that a Section 2703 warrant involves a "threat to individual privacy," *id.* at 49a, pointing out that a judge's probable-cause finding afforded "the highest level of protection" under the Fourth Amendment. *Id.* at 50a. And he reasoned that because a Section 2703 warrant "does not operate like a traditional arrest or search warrant," the majority's conclusion that such a warrant invades privacy in the location where "private content is stored" was "suspect." *Id.* at 62a n.6, 65a n.7. He nevertheless concurred in the judgment, despite "considerable" hesitation, on the ground that Congress did not "demonstrate[] a clear intention to reach situations" in which data is stored abroad. *Id.* at 66a-67a; see *id.* at 65a n.7. He made clear, however, that he harbored no "illusion that" the court's holding "should * * * be regarded as a rational policy outcome, let alone celebrated as a milestone in protecting privacy." *Id.* at 72a.

4. The government petitioned for rehearing en banc. By an evenly divided 4-4 vote, with several judges

recused and Judge Lynch ineligible to participate because he had recently taken senior status, the court of appeals denied the petition. See Pet. App. 105a & n.*, 107a n.1. Judge Carney, who authored the panel's decision, concurred in the denial of rehearing to reiterate the panel's reasoning. See *id.* at 107a-119a. Judges Jacobs, Cabranes, Raggi, and Droney each dissented from the denial (and joined each other's dissents). See *id.* at 120a-154a. References to "dissenting" opinions in this brief are to the dissents from the denial of rehearing en banc.

a. Judge Jacobs explained that a Section 2703 warrant "functions as a subpoena." Pet. App. 120a. Thus, he observed, "[e]xtraterritoriality need not be fussed over when the information sought is already within the grasp of a domestic entity served with a warrant." *Id.* at 121a. Even assuming that the relevant statutory focus is "user privacy," Judge Jacobs found the panel's focus on the location of data storage both "unmanageable" and "increasingly antiquated." *Id.* at 121a-122a. In his view, "[t]he warrant in this case can reach what it seeks because the warrant was served on Microsoft," and Microsoft "need only touch some keys in Redmond, Washington" to "access * * * the information sought." *Id.* at 121a.

b. Judge Cabranes likewise questioned how this application of Section 2703 could be considered extraterritorial. Pet. App. 124a. Even assuming that the relevant statutory focus is "user privacy," he reasoned that "a plain reading of the statute makes clear that the conduct relevant to" that focus "is a provider's *disclosure* or *non-disclosure* of emails to third parties, not a provider's *access* to a customer's data." *Id.* at 132a. Judge

Cabranes pointed out that the SCA recognizes a provider's right to access a user's communications, that such access does not invade a user's privacy unless the provider discloses the communications to someone else, and that Microsoft has lawful possession of the relevant emails and the ability to access those emails from its U.S. headquarters. *Id.* at 129a n.19, 135a-136a. Because disclosure of the emails to the government would take place in the United States, Judge Cabranes concluded, enforcement of the warrant in this case is a permissible domestic application of Section 2703. *Id.* at 136a; see *id.* at 132a.

Judge Cabranes also detailed a number of "far reaching," harmful effects of the panel's decision. Pet. App. 125a. First, the decision "has substantially burdened the government's legitimate law enforcement efforts" by preventing enforcement of a warrant requiring a service provider to "turn over emails stored in servers located outside the United States," even if the government is certain that the emails contain evidence of a "terrorist plot" or other serious criminal wrongdoing. *Id.* at 125a-126a (citation omitted). Second, the decision has "created a roadmap for the facilitation of criminal activity," because it allows even an "unsophisticated" criminal in the United States to shield emails from the government's view by falsely reporting a foreign residence when signing up for a Microsoft email service. *Id.* at 125a-127a. Third, the decision has "impeded programs to protect the national security of the United States and its allies" by leading "major service providers to reduce significantly their cooperation with law enforcement." *Id.* at 125a, 127a-128a.

c. Judge Raggi agreed with Judge Jacobs and Judge Cabranes that the panel's extraterritoriality analysis is

flawed, even assuming that Section 2703 focuses on "privacy," because privacy is not invaded by "Microsoft's access of its own files in Dublin." Pet. App. 147a. Rather, any invasion of privacy occurs only upon the "subsequent disclosure of subscriber communications in the United States." *Ibid.*; see *id.* at 145a. That is particularly true, she explained, because Microsoft does not "'seiz[e]' anything as an agent of the government" under Section 2703. *Id.* at 144a. In her view, "Microsoft did not need any warrant from the United States to take possession of the subscriber communications it had stored in Ireland" or "to transfer those communications from Ireland to the United States." *Id.* at 145a. Only Microsoft's disclosure of the communications to the government represented an action that "would otherwise have been prohibited" absent the Section 2703 warrant. *Ibid.*

d. Judge Droney echoed the analysis in the other dissents. He also stressed that, in performing an extraterritoriality analysis, "a court must read the statute provision by provision, not as a whole." Pet. App. 151a. He explained that Section 2703's provisions "concerning the means of disclosure following obtaining the warrant are quite separate from the privacy components of the SCA." *Id.* at 152a. Because "Microsoft is headquartered in the United States," he continued, "there is no question that it would make the disclosure mandated by the [Section] 2703 warrant in this country." *Ibid.*

SUMMARY OF ARGUMENT

Under 18 U.S.C. 2703, the government may compel a U.S. service provider to disclose electronic communications within its control, regardless of whether the provider stores those communications in the United States or abroad.

A. Applying Section 2703 to require the disclosure of data stored abroad does not violate the presumption against extraterritoriality. Even where that presumption is unrebutted, a court must examine whether "the conduct relevant to the statute's focus occurred in the United States." *RJR Nabisco, Inc.* v. *European Cmty.*, 136 S. Ct. 2090, 2101 (2016). The focus turns on the acts that the statutory provision "seeks to regulate" and the parties or interests that it "seeks to protect." *Morrison* v. *National Austl. Bank Ltd.*, 561 U.S. 247, 267 (2010) (brackets, citation, and internal quotation marks omitted). The focus inquiry is provision-specific; the focus of Section 2703 need not be the same as other provisions of the SCA or the ECPA. See *RJR Nabisco*, 136 S. Ct. at 2103, 2106.

The focus of Section 2703 is on domestic conduct: the disclosure of electronic records to the government in the United States. Congress captioned that provision "Required disclosure of customer communications or records." Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 (Patriot Act), Pub. L. No. 107-56, Tit. II, § 212(b), 115 Stat. 284-285 (emphasis omitted). Section 2703's text accordingly describes the multiple mechanisms by which the government can "require the disclosure" of electronic records. 18 U.S.C. 2703(a); see 18 U.S.C. 2703(b) ("governmental entity may require a provider * * * to disclose"); 18 U.S.C. 2703(c) ("governmental entity may require a provider * * * to disclose"). The legislative history underscores that Congress sought to regulate providers' disclosure of electronic information to the government, not providers' storage of that information. And because any disclosure to the government occurs in

the United States, such disclosure involves a permissible domestic application of Section 2703.

The court of appeals took a different view, concluding that the "focus" of the SCA is "user privacy." Pet. App. 43a. Even if that were correct, any invasion of privacy occurs in the United States. Microsoft does not invade a user's privacy when it transfers data from an Irish server to a U.S. server, or vice versa. A user has no right under the SCA to have his data stored in one location or another, or even to know where it is stored. Instead, any invasion of privacy occurs only when Microsoft divulges a user's communications to the government and the government examines those communications for evidence of a crime.

B. The conclusion that a Section 2703 warrant compels U.S. providers to disclose foreign-stored data comports with common-law principles that were well established when Congress enacted the SCA. Courts have long held that "[t]he test for the production of documents is control, not location." *Marc Rich & Co.* v. *United States*, 707 F.2d 663, 667 (2d Cir.), cert. denied, 463 U.S. 1215 (1983). Thus, a subpoena recipient in the United States is required to disclose requested records regardless of whether the recipient has chosen to store those records abroad. See *id.* at 667-668.

The same rule applies to Section 2703 warrants. Although those devices are warrants in the sense that they require the government to demonstrate probable cause under oath before a neutral magistrate judge and state with particularity the items to be searched, they are executed like subpoenas. Rather than authorizing law enforcement officers to physically enter private premises, a Section 2703 warrant authorizes the gov-

ernment to "require the disclosure by a provider of electronic communications." 18 U.S.C. 2703(a); see 18 U.S.C. 2703(b) and (c). In practice, then, the statutory requirement to disclose records pursuant to a Section 2703 warrant operates like the execution of a subpoena: The government serves a demand for records on a person who controls the potential evidence. Just as a subpoena requires the recipient to produce material stored abroad that is within the recipient's control, so too does a Section 2703 warrant. Congress did not incongruously grant the government access to less information when it employs a Section 2703 warrant than when it employs Section 2703's other disclosure mechanisms.

C. A more restrictive reading of Section 2703 would undermine an important tool for law enforcement and introduce arbitrariness to the statutory scheme. Because Microsoft gives dispositive weight to the location of data, a provider could move all information about U.S. subscribers beyond the reach of U.S. law enforcement simply by building its servers outside the United States. Or it could follow other major providers, such as Google, which move data all over the world, sometimes breaking it into "shards" so that different portions of a single email account may be stored in multiple countries at any one moment. Even though such providers can access information from their offices in the United States, Microsoft's data-location theory would erect an insurmountable barrier to U.S. law enforcement's securing of critical evidence.

D. In response, Microsoft argues that its theory is necessary to avoid international discord. That concern is overstated. Many other countries construe their laws to authorize compelling domestic entities to produce

foreign-stored evidence, even if they place varying restrictions on the use of that power. Indeed, the United States is a party to a treaty that requires parties to have the power to compel service providers within their territory to produce data under the providers' control for law enforcement purposes. And to the extent Microsoft worries that it will be subject to conflicting legal regimes at home and abroad, that situation has not often arisen and can be addressed through existing mechanisms if it does. In any event, it provides no basis for overriding the best reading of the statutory scheme.

ARGUMENT

UNDER 18 U.S.C. 2703, THE GOVERNMENT MAY REQUIRE A U.S. SERVICE PROVIDER TO DISCLOSE ANY ELECTRONIC COMMUNICATONS WITHIN ITS CONTROL

The government's request for records in this case complies with the text of 18 U.S.C. 2703: Microsoft is a service "provider" that sends and stores electronic communications, and the government has "require[d]" the disclosure of those communications by obtaining "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure." 18 U.S.C. 2703(a), (b)(1), and (c)(1)(A). Microsoft does not dispute any of that. Instead, it invokes the presumption against extraterritoriality, arguing that Congress did not intend Section 2703 to apply when a U.S. service provider stores electronic communications abroad. Pet. App. 21a. Although Microsoft is correct that the presumption against extraterritoriality applies to Section 2703 and is unrebutted, it is incorrect that this case involves an extraterritorial application of that statutory provision.

"It is a basic premise of our legal system that, in general, 'United States law governs domestically but does

not rule the world.'" *RJR Nabisco, Inc.* v. *European Cmty.*, 136 S. Ct. 2090, 2100 (2016) (quoting *Microsoft Corp.* v. *AT&T Corp.*, 550 U.S. 437, 454 (2007)). Thus, "[a]bsent clearly expressed congressional intent to the contrary, federal laws will be construed to have only domestic application." *Id.* at 2100 (citing *Morrison* v. *National Austl. Bank Ltd.*, 561 U.S. 247, 255 (2010)). This Court has outlined "a two-step framework for analyzing extraterritoriality issues." *Id.* at 2101. At the first step, courts "ask whether the presumption against extraterritoriality has been rebutted" by a "clear, affirmative indication that [the statutory provision] applies extraterritorially." *Ibid.* If the presumption is unrebutted and "the statute is not extraterritorial," courts decide at step two "whether the case involves a domestic application of the statute * * * by looking to the statute's 'focus.'" *Ibid.* "If the conduct relevant to the statute's focus occurred in the United States, then the case involves a permissible domestic application even if other conduct occurred abroad." *Ibid.*

This case involves the second step. The sole question is whether the conduct relevant to Section 2703's focus occurs in the United States. It does: Section 2703 focuses on disclosure, and the disclosure of records from Microsoft to the government would occur in the United States. Even if the statutory focus were "user privacy," any incursion on a user's privacy would occur not when Microsoft collects materials already in its possession but when it turns over those materials to law enforcement personnel in the United States. Other relevant factors—the common-law background, practical implications, and international obligations—support the same conclusion: Compliance with a Section 2703 warrant is a domestic, not an extraterritorial, act.

A. This Case Involves A Domestic Application Of Section 2703

1. This Court's decisions require a provision-specific "focus" analysis

A court ascertains the focus of a particular statutory provision by identifying the acts that the provision "seeks to 'regulate'" and the parties or interests that it "seeks to 'protec[t].'" *Morrison*, 561 U.S. at 267 (quoting *Superintendent of Ins. of N.Y.* v. *Bankers Life & Cas. Co.*, 404 U.S. 6, 10, 12 (1971)); see *RJR Nabisco*, 136 S. Ct. at 2100-2101. Because a different section (or even a different subsection) of the same enactment may have a different focus, the analysis must proceed on a provision-by-provision basis.

The Court applied such a provision-specific extraterritoriality analysis in *RJR Nabisco*. That decision considered the extraterritoriality of 18 U.S.C. 1962, a substantive provision proscribing certain racketeering conduct, and 18 U.S.C. 1964, a civil damages provision stating that "[a]ny person injured in his business or property" by reason of a violation of the Racketeer Influenced and Corrupt Organization Act (RICO), 18 U.S.C. 1961 *et seq.*, may bring suit. 136 S. Ct. at 2099-2100 (brackets in original). The Court held that Section 1962 applies extraterritorially "to the extent that the predicates alleged in a particular case themselves apply extraterritorially." *Id.* at 2102. It noted that its conclusion was "determinative" for two subsections, Section 1962(b) and (c). *Id.* at 2103. But it reserved judgment on whether two other subsections, Section 1962(a) and (d), shared the same extraterritorial reach. *Ibid.*

The Court then assessed Section 1964 in a different section of its opinion. It concluded that Section 1964 does not apply extraterritorially; it instead "requires a

civil RICO plaintiff to allege and prove a domestic injury to business or property." *RJR Nabisco*, 136 S. Ct. at 2111. The Court thus implicitly determined that the injury itself, and not the conduct that caused the injury, is the focus of Section 1964. See *id.* at 2108 (noting that "[i]t is not enough" that "the underlying law governs conduct in foreign countries"); *id.* at 2111 (asking "whether a particular alleged injury is 'foreign' or 'domestic'"). In distinguishing Section 1962, the Court emphasized that the extraterritoriality analysis "must be applied separately" to the various statutory provisions. *Id.* at 2108; see *id.* at 2106 ("Irrespective of any extraterritorial application of § 1962, we conclude that § 1964(c) does not overcome the presumption against extraterritoriality."). That makes good sense, the Court observed, because different provisions could pose different risks of "international friction." *Ibid.*

The Court similarly conducted a provision-specific analysis in *Morrison*. There, the Court discussed Section 10(b) of the Securities Exchange Act of 1934, 15 U.S.C. 78j(b), which makes it unlawful to "use or employ, in connection with the purchase or sale of any security registered on a national securities exchange * * * [,] any manipulative or deceptive device or contrivance in contravention of" SEC rules and regulations. The Court held that the "focus" of Section 10(b) is "purchases and sales of securities in the United States," not "the place where the deception originated." *Morrison*, 561 U.S. at 266. That is, transactions on domestic exchanges, and domestic transactions in other securities, are "the objects of the statute's solicitude." *Id.* at 267. But the Court did not assume that the same was true for other provisions of the Securities Exchange Act. To

the contrary, it observed that Section 30(a) of the statute, 15 U.S.C. 78dd(a), applies extraterritorially. *Morrison*, 561 U.S. at 265.

Since *Morrison* and *RJR Nabisco*, lower courts correctly have assessed the focus of the specific statutory provision at issue, not the statute as a whole. See *Loginovskaya* v. *Batratchenko*, 764 F.3d 266, 272-273 (2d Cir. 2014) (concluding that the focus of one provision is "clearly transactional," while acknowledging that a separate provision of the same statute has an "apparent focus on the persons who are regulated without regard to where the resulting transaction occurs"); *TianRui Grp. Co.* v. *International Trade Comm'n*, 661 F.3d 1322, 1329 (Fed. Cir. 2011) (concluding that the "focus" of a particular statutory provision is "on the act of importation and the resulting domestic injury"); *United States* v. *All Assets Held at Bank Julius*, 251 F. Supp. 3d 82, 99 (D.D.C. 2017) (identifying the provision's focus by looking to its specific text and legislative history); cf. *United States* v. *Ballestas*, 795 F.3d 138, 144 (D.C. Cir. 2015) (noting that "the extraterritorial reach of a particular provision will not necessarily be imputed to an entire statute"), cert. denied, 136 S. Ct. 1229 (2016); *Liu Meng-Lin* v. *Siemens AG*, 763 F.3d 175, 179-181 (2d Cir. 2014) (rejecting the argument that all provisions of a statutory scheme must apply extraterritorially).

In assessing the entire SCA, or perhaps even the entire ECPA, the court of appeals thus aimed at the wrong target. See Pet. App. 37a-38a (emphasizing that Section 2703 "appears in a statute entitled the Electronic Communications Privacy Act"); *id.* at 39a (explaining that Section 2701 "protects the privacy interests of users"); *ibid.* (stating that "[t]he primary obligations created by the SCA protect the electronic communications"); *id.* at

41a-42a (citing general comments about privacy from the ECPA's legislative history). An appropriately tailored extraterritoriality analysis should instead identify the focus of Section 2703 itself. The focus of that provision—which governs the disclosure of wire and electronic communications to domestic law enforcement officers, see 18 U.S.C. 2703—need not extend to other parts of the SCA, or vice versa.

2. Section 2703 focuses on the disclosure of electronic communications in the United States

Section 2703 focuses on a provider's disclosure of electronic communications to the government, and that disclosure occurs in the United States. The text of Section 2703 and the relevant legislative history point to that same result. Consistent with that interpretation, every judge to have issued a written opinion on the question since the decision below has determined that the relevant conduct—that is, the conduct falling within Section 2703's focus—occurs in the United States.[2]

---

[2] See *United States* v. *Google, Inc.*, No. 17-mc-7 (W.D. Tenn. Nov. 3, 2017) (sealed); *In re Search Warrant Issued to Google, Inc.*, No. 17-mj-532, 2017 WL 4022806, at *9 (N.D. Ala. Sept. 1, 2017); *In re the Matter of the Search of Information Associated with [REDACTED]@gmail.com that is stored at premises controlled by Google*, No. 17-7131 (D. Ariz. Aug. 21, 2017); *In re Search Warrant No. 16-960-M-1 to Google*, No. 16-960, 2017 WL 3535037, at *11 (Aug. 17, 2017), aff'g 232 F. Supp. 3d 708 (E.D. Pa. Feb. 3, 2017); *In re the Search of Content Stored at Premises Controlled by Google Inc.*, No. 16-mc-80263, 2017 WL 3478809, at *5 (Aug. 14, 2017), aff'g 2017 WL 1487625 (N.D. Cal. Apr. 25, 2017); *In re Search of Information Associated with [Redacted]@gmail.com That is Stored at Premises Controlled by Google, Inc.*, No. 16-mj-757, 2017 WL 3445634, at *27 (July 31, 2017), aff'g 2017 WL 2480752 (D.D.C. June 2, 2017); *In re Search of Information Associated with Accounts Identified as [redacted]@gmail.com*, No. 16-mj-2197, 2017 WL

a. The text of Section 2703 makes clear that the provision focuses on disclosure. That is immediately apparent from Section 2703's heading: "Required disclosure of customer communications or records." Patriot Act § 212, 115 Stat. 284-285; see *Yates* v. *United States*, 135 S. Ct. 1074, 1083 (2015) (plurality opinion) (relying in part on headings to discern statutory meaning). The body of Section 2703 then defines the various circumstances under which the government can "require the disclosure" of the contents of electronic communications, or of other records relating to such communications, pursuant to a warrant, a 2703(d) order, or a subpoena. 18 U.S.C. 2703(a); see 18 U.S.C. 2703(b) ("governmental entity may require a provider * * * to disclose"); 18 U.S.C. 2703(c) ("governmental entity may require a provider * * * to disclose"). Although the three statutory mechanisms implicate different showings and reach different classes of records, the end result of each mechanism is the same: disclosure from a provider to the government.

If the government obtains a warrant, as it did here, it may require the disclosure of several types of information. The government "may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication"; "may

---

3263351, at *9 (C.D. Cal. July 13, 2017); *In re Search Warrant to Google, Inc.*, No. 16-4116, 2017 WL 2985391, at *12 (D.N.J. July 10, 2017); *In re Two Email Accounts Stored at Google, Inc.*, No. 17-M-1235, 2017 WL 2838156, at *4 (E.D. Wis. June 30, 2017); *In re Search of Premises Located at [Redacted]@yahoo.com*, No. 17-mj-1238 (M.D. Fla. Apr. 7, 2017), slip op. 3; *In re Information Associated with One Yahoo Email Address That Is Stored at Premises Controlled by Yahoo*, No. 17-M-1234, 2017 WL 706307, at *3 (E.D. Wis. Feb. 21, 2017).

require a provider of remote computing service to disclose the contents" of certain communications; and "may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber." 18 U.S.C. 2703(a)-(c). Section 2703 also contains several other procedures regulating disclosure under a Section 2703 warrant. For example, the statute protects providers from suit for "providing information" under a disclosure order. 18 U.S.C. 2703(e). It also mandates that providers preserve electronic communications at the government's request, so that the material will be available for later disclosure to the government. 18 U.S.C. 2703(f). And it states that the presence of an officer is not required for service or execution of a warrant "requiring disclosure." 18 U.S.C. 2703(g).

All told, Section 2703 regulates "disclosure," "disclosing," or the requirement to "disclose" a dozen times throughout the provision. By comparison, it mentions "storage" only in describing the category of communications covered by the statute. See 18 U.S.C. 2703(a). The statute does not prescribe where a service provider must store emails, or how long it must retain them, or under what conditions it must store them, or with what technology it must safeguard them. Thus, although the disclosure rules apply to stored electronic communications, Section 2703 regulates their disclosure—not their storage. By repeatedly emphasizing the disclosure from a provider to the government, the text of Section 2703 indicates that the provision "seeks to 'regulate'" disclosure to the government and "to 'protec[t]'" the government's interest in obtaining such disclosure. *Morrison*, 561 U.S. at 267 (quoting *Superintendent of Ins. of N.Y.*, 404 U.S. at 10, 12).

b. The legislative history supports the conclusion that Section 2703 focuses on the disclosure of information to the government. That is true both of the original SCA and of its significant amendments in 2001.

In connection with the 1986 enactment of the SCA, the relevant Senate Report described Section 2703 as "provid[ing] requirements for the government to obtain the contents of an electronic communication that has been in electronic storage for 180 days or less." S. Rep. No. 541, 99th Cong., 2d Sess. 38 (1986). Similarly, the House Report explained that Section 2703 "contains the procedural requirements for the government to obtain access to electronic communications in storage and transactional records relating thereto," and noted that Section 2703(a) "sets forth the requirements which must be met before the government may obtain access to the contents" of electronic communications. H.R. Rep. No. 647, 99th Cong., 2d Sess. 67 (1986). Consistent with those understandings, Congress originally captioned Section 2703 "Requirements for governmental access." ECPA § 201, 100 Stat. 1861. Those data points underscore that Section 2703 focuses on the government's acquisition of information from a provider—not a provider's storage of that information.

Congress later amended Section 2703 as part of the Patriot Act. Among other things, Congress changed the provision's heading from "Requirements for governmental access" to "Required disclosure of customer communications or records." Patriot Act § 212(b), 115 Stat. 285 (emphasis omitted). Moreover, that amendment to Section 2703 appeared in a section of the Patriot Act captioned "Emergency disclosure of electronic communications to protect life and limb." *Id.* § 212, 115 Stat. 284 (capitalization altered; emphasis omitted).

Those additional markers in the legislative history confirm that Congress has consistently understood Section 2703 to focus on the disclosure of information to the government.

* * *

Because the "conduct relevant to [Section 2703's] focus" occurs in this country, the existence of some "other conduct" that "occur[s] abroad" does not alter the conclusion that this case "involves a permissible domestic application" of that provision. *RJR Nabisco*, 136 S. Ct. at 2101. Here, the Section 2703 warrant requires a provider incorporated and subject to process in the United States to disclose records to the U.S. government in the United States, based on probable cause to believe that the specified records include evidence of crime in the United States. See J.A. 22. As the magistrate judge who issued the warrant observed, that application of Section 2703 "does not criminalize conduct taking place in a foreign country; it does not involve the deployment of American law enforcement personnel abroad; it does not require even the physical presence of service provider employees at the location where data are stored." Pet. App. 92a.

Indeed, Microsoft could comply with the warrant by undertaking acts entirely within the United States. As the court of appeals acknowledged, "by using a database management program that can be accessed at some of its offices in the United States, [Microsoft] can 'collect' account data that is stored on any of its servers globally and bring that data into the United States." Pet. App. 8a (citation omitted); see J.A. 33-34 (testimony that Microsoft's "Global Criminal Compliance (GCC) team is responsible for handling" responses to law enforcement requests for emails and that "[t]he GCC team works

from offices in the United States"). At most, Microsoft need only take the initial step of "collect[ing]" data stored abroad by inputting commands at its facility in the United States. J.A. 34; see Pet. App. 45a (noting that Microsoft must "interact with the Dublin datacenter"). That single preparatory step is not "the conduct relevant to the statute's focus." *RJR Nabisco*, 136 S. Ct. at 2101. Because Section 2703 focuses on the domestic disclosure of information to the government, this case involves a permissible domestic application of the statute.

3. Even if Section 2703 focuses on privacy, any invasion of privacy occurs in the United States

The court of appeals nevertheless determined that the SCA generally "focuses on user privacy" and that any "invasion of the customer's privacy takes place under the SCA where the customer's protected content is accessed," apparently meaning where that data is stored. Pet. App. 43a; see *id.* at 44a. But even assuming that a more general focus of the SCA or the ECPA should be imputed to Section 2703, and that Section 2703 thus focuses on "user privacy," the relevant invasion of privacy occurs in the United States, when Microsoft discloses information to the government and the government reviews that information. Accordingly, identifying "privacy" as the focus of Section 2703 leads to the same conclusion as identifying "disclosure" as the statutory focus: Compliance with a Section 2703 warrant requiring disclosure of information in the United States is a domestic, not an extraterritorial, act.

a. Privacy "is an abstract concept with no obvious territorial locus." Pet. App. 65a n.7 (Lynch, J., concurring in the judgment); see *id.* at 121a (Jacobs, J., dissenting) ("[P]rivacy, which is a value or a state of mind,

lacks location."). To the extent the SCA protects privacy, it does so by shielding stored electronic communications from the eyes of someone other than the service provider. See 18 U.S.C. 2701(a) (prohibiting unauthorized persons from "obtain[ing] * * * access to" electronic communications); 18 U.S.C. 2702(a) (restricting providers from "knowingly divulg[ing]" the contents of electronic communications). But any statutory privacy protections do not prohibit a *provider* from moving a user's data to another server here or abroad. Cf. 18 U.S.C. 2701(c)(1) (excluding from Section 2701's bar on unlawful access any conduct authorized "by the person or entity providing a wire or electronic communications service"); 18 U.S.C. 2702(b)(4)-(5) (exempting certain provider activities from Section 2702's bar on knowing disclosures); 18 U.S.C. 2702(c)(3) (same).

Thus, Microsoft does not invade a user's privacy by transferring data from its servers in Ireland to a server in the United States. Just as Microsoft was not restricted from migrating the specified account from the United States to Ireland in the first instance, it is not restricted from migrating the account back to the United States. See J.A. 30-31. It does not need authorization to do so; it already has custody and control of the targeted communications and the legal ability to move them at will. The user of Microsoft's services has no recourse under U.S. law, or even entitlement to notice, if Microsoft decides to transfer her stored communications into or out of the United States. See Pet. App. 144a-145a, 147a (Raggi, J., dissenting) (Microsoft "did not need the approval * * * of its subscriber to take such action."). The user simply lacks a "privacy" interest vis-à-vis Microsoft as to the location of her stored communications.

b. Rather, any invasion of a user's privacy occurs only when Microsoft discloses the communications to a third party (other than the intended recipient). That is why Section 2702 outlines the precise circumstances in which a provider may "knowingly divulge to any person or entity the contents of a communication." 18 U.S.C. 2702(a)(1); see 18 U.S.C. 2702(b)(2) and (c)(1). The use of the term "divulge" indicates that the provider's control over stored communications is not the concern; a potential privacy invasion occurs only when the provider shares the communications that are in its lawful custody and control with an unauthorized third party.

Under Section 2703, the provider must disclose information to the government under one of three separate mechanisms. See 18 U.S.C. 2703(a)-(c). That disclosure to the government—paired with the government's subsequent review of a user's emails for information relating to criminal activity—is the only act that invades a user's privacy. And again, that act occurs in the United States, not in the foreign country or countries where Microsoft may decide to store the user's emails at any given moment.

Importantly, the existence of a probable-cause-based warrant justifies any invasion of privacy effected by the government's acquisition and review of the user's communications. As this Court recently explained, warrants "protect privacy in two main ways." *Birchfield* v. *North Dakota*, 136 S. Ct. 2160, 2181 (2016). First, a warrant ensures that "a neutral magistrate makes an independent determination that there is probable cause to believe that evidence will be found." *Ibid.* Second, "the warrant limits the intrusion on privacy by specifying the scope of the search." *Ibid.* The Section 2703 warrant here satisfies both of those concerns.

c. In determining that Microsoft's compliance with the Section 2703 warrant would create an extraterritorial violation of privacy, the court of appeals relied on the determination that Microsoft "seize[s]" information in Ireland "as an agent of the government." Pet. App. 43a-44a. As explained below, that determination is doubly flawed. First, parties who comply with orders to disclose information—typically, subpoenas or summonses—have not been characterized as government agents. Second, even if Microsoft were an agent, it is not conducting any search or seizure in Ireland by transferring material that is stored on a server there, and that Microsoft is free to move among storage facilities at any time, to a server in Washington.

i. When the government compels a private actor to conduct a search or seizure, the private actor can function as an agent of the government for purposes of the Fourth Amendment. See *Skinner* v. *Railway Labor Execs.' Ass'n*, 489 U.S. 602, 614-615 (1989). Such an agency relationship arises only where the private actor affirmatively invades a privacy interest at the government's behest. See, *e.g.*, *id.* at 614-616 (assessing whether railroads acted as government agents in administering drug tests in compliance with federal regulations); *Gambino* v. *United States*, 275 U.S. 310, 314-317 (1927) (assessing whether state troopers acted as federal agents in seizing liquor).

By contrast, where a private actor merely gathers information stored in its own files, it does not function as a government agent. This Court has rejected the argument that a private bank's compliance with record-keeping requirements for transactions to which the bank itself is a party transforms the bank into a govern-

ment agent that is "seiz[ing]" the records of its customers. See *California Bankers Assn.* v. *Shultz*, 416 U.S. 21, 52-54 (1974). And it has never suggested that a person who complies with a subpoena or a summons becomes a government agent simply by collecting and producing the evidence in its possession. Rather, the subpoena recipient functions in a private capacity as a witness, which is why a recipient can assert Fourth and (if applicable) Fifth Amendment rights. See *Donovan* v. *Lone Steer, Inc.*, 464 U.S. 408, 414 (1984) (Fourth Amendment); *United States* v. *Hubbell*, 530 U.S. 27, 35-37 (2000) (Fifth Amendment). A subpoena for records, just as a subpoena for testimony, rests on "the general common-law principle that the public has a right to every man's evidence." *Kastigar* v. *United States*, 406 U.S. 441, 443 (1972) (citation and internal quotation marks omitted).

ii. Even if Microsoft functions as a government agent in disclosing the information that a Section 2703 warrant requires, it does not perform either a "seizure" or a "search" in Ireland when it transfers material stored on a server in another country to its offices in the United States. For purposes of the Fourth Amendment, a "seizure" of property occurs where "there is some meaningful interference with an individual's possessory interests in that property." *Soldal* v. *Cook Cnty.*, 506 U.S. 56, 63 (1992) (quoting *United States* v. *Jacobsen*, 466 U.S. 109, 113 (1984)). As this Court has explained, that definition of the "seizure" of property "follows from [the Court's] oft-repeated definition of the 'seizure' of a person within the meaning of the Fourth Amendment—meaningful interference, however brief, with an individual's freedom of movement." *Jacobsen*, 466 U.S. at 113 n.5; see, *e.g.*, *California* v. *Hodari D.*,

499 U.S. 621, 624 (1991) ("From the time of the founding to the present, the word 'seizure' has meant a 'taking possession.'") (citations omitted).

Under that settled definition, a provider does not "seize" records when it collects and transfers materials that are already in its custody and control and that it remains free to move among storage facilities at any time. When Microsoft transfers information from its datacenter in Dublin to its offices in the United States, it neither "interfere[s] with" a user's "possessory interests" in his emails, *Soldal*, 506 U.S. at 63 (citation omitted), nor expands its authority over those emails. And even if the subsequent disclosure of the emails to the government could be deemed a "seizure" that interferes with the user's possessory interests, that disclosure takes place in the United States.

Nor do Microsoft's actions abroad constitute a "search." A "search" is an infringement on "an expectation of privacy that society is prepared to consider reasonable." *Jacobsen*, 466 U.S. at 113. Microsoft does not offend any reasonable expectation of privacy when it transfers material from a server in Dublin to its domestic offices—a transfer that Microsoft is free to perform at any time in the conduct of its business. And assuming that a user has a reasonable expectation of privacy in the contents of her emails, the Section 2703 warrant here did not deputize Microsoft to perform a search of those contents. The warrant left to law enforcement the task of reviewing those emails to determine whether they "constitute[] fruits, evidence and instrumentalities" of a crime. J.A. 25; compare J.A. 24 (warrant provision requiring Microsoft to disclose "all e-mails stored in the account"), with J.A. 25 (warrant provision permitting government officials "to search

the seized e-mails for evidence of the specified crimes"). As a result, any search occurs, at the earliest, when government authorities receive communications from a provider—which, again, takes place in the United States, not Ireland.

B. Congress Enacted Section 2703 Against The Background Principle That Subpoena Recipients Must Produce All Records Within Their Control

When Congress enacted the SCA in 1986, it did so against a backdrop of settled law about the execution of subpoenas. Under longstanding principles, the recipient of a subpoena to produce documents in the United States must produce all specified materials within its control, even if the recipient chooses to store those materials abroad. This Court should presume that Congress was aware of, and did not intend to abrogate, those well-established principles when it crafted Section 2703 to require disclosure under subpoenas, court orders, and warrants. See *Kirtsaeng* v. *John Wiley & Sons, Inc.*, 568 U.S. 519, 538 (2013) ("When a statute covers an issue previously governed by the common law, we must presume that Congress intended to retain the substance of the common law.") (brackets, citation, and internal quotation marks omitted).

1. In enforcing subpoenas, courts have focused on their jurisdiction over the subpoena *recipient*, not the location of the requested *records*. See 9A Charles Alan Wright & Arthur R. Miller, *Federal Practice and Procedure* § 2456, at 417 (3d ed. 2008) ("The case law clearly has established that even records kept beyond the territorial jurisdiction of the district court issuing the subpoena may be covered if they are controlled by someone subject to the court's jurisdiction."); *Hay Grp., Inc.* v. *E.B.S. Acquisition Corp.*, 360 F.3d 404, 412 (3d Cir.

2004) (Alito, J.) (explaining that subpoenaed documents are produced "not [in] the district in which the documents are housed but [in] the district in which the subpoenaed party is required to turn them over"). That is because "[t]he test for the production of documents is control, not location." *Marc Rich & Co.* v. *United States*, 707 F.2d 663, 667 (2d Cir.), cert. denied, 463 U.S. 1215 (1983).

Courts of appeals have long applied that general rule to subpoenas for documents stored abroad. As those courts have explained, a subpoena requiring a company doing business in the United States to produce records is enforceable regardless of whether the company must retrieve those records from outside the country. See, *e.g.*, *In re Sealed Case*, 832 F.2d 1268, 1270, 1283-1284 (D.C. Cir. 1987) (concluding that a subpoena for documents in Switzerland is enforceable if the district court has personal jurisdiction over the companies whose records are sought), abrogated on other grounds by *Braswell* v. *United States*, 487 U.S. 99 (1988); *United States* v. *Bank of Nova Scotia*, 740 F.2d 817, 820-821, 826-829 (11th Cir. 1984) (affirming order enforcing grand jury subpoena requiring a foreign bank subject to the jurisdiction of the district court to disclose records located in the Bahamas), cert. denied, 469 U.S. 1106 (1985); *Marc Rich & Co.*, 707 F.2d at 667-668 (holding that "service of a subpoena upon [a company's] officers within the territorial boundaries of the United States would be sufficient to warrant judicial enforcement," regardless of whether "the documents are located abroad"); *United States* v. *First Nat'l City Bank*, 396 F.2d 897, 900-901, 905 (2d Cir. 1968) (affirming contempt finding against American bank that refused to comply with sub-

poena for documents held in its German office); *Securities and Exchange Comm'n* v. *Minas de Artemisa*, 150 F.2d 215, 218 (9th Cir. 1945) ("The obligation to respond applies even though the person served [with a subpoena] may find it necessary to go to some other place within or without the United States in order to obtain the documents required to be produced."); see also *Société Nationale Industrielle Aérospatiale* v. *United States Dist. Court*, 482 U.S. 522, 539-540 (1987) (explaining that a treaty establishing optional procedures for obtaining evidence abroad "did not deprive the District Court of the jurisdiction it otherwise possessed to order a foreign national party before it to produce evidence physically located within a signatory nation"). Thus, at the time that Congress enacted the SCA, it was "no longer open to doubt that a federal court has the power to require the production of documents located in foreign countries if the court has *in personam* jurisdiction of the person in possession or control of the material." *First Nat'l City Bank*, 396 F.2d at 900-901.

2. Applying Section 2703 to reach electronic communications stored abroad is consistent with that settled law on the execution of subpoenas. Although Congress labeled the Section 2703 mechanism at issue a "warrant," 18 U.S.C. 2703(a) and (b)(1)(A), that label primarily indicates the level of *suspicion* necessary to demand the disclosure of a provider's records. Congress used the term "warrant" because the statute requires the government to demonstrate to a neutral judicial officer facts showing probable cause—a privacy protection of the highest order. In its *execution*, however, the requirement to disclose under a Section 2703 warrant "functions as a subpoena." Pet. App. 120a (Jacobs, J.,

dissenting); see *id.* at 130a n.19 (Cabranes, J., dissenting) (a "disclosure warrant is more akin to a subpoena"); *id.* at 140a-141a (Raggi, J., dissenting) ("a [Section] 2703(a) warrant is not a traditional warrant"); *id.* at 58a (Lynch, J., concurring in the judgment) (a Section 2703 warrant is not a "traditional search warrant"). That is so for three reasons.

First, a traditional search warrant authorizes law enforcement officers to search private premises and to seize materials from those premises. See *Donovan*, 464 U.S. at 414 (explaining that search warrants authorize "nonconsensual entries into areas not open to the public"). That is, "[s]earch warrants are not directed at persons; they authorize the search of 'places' and the seizure of 'things.'" *Zurcher* v. *Stanford Daily*, 436 U.S. 547, 555 (1978) (brackets and citation omitted). Under Federal Rule of Criminal Procedure 41, a search warrant is issued "to an officer authorized to execute it," and "[a]n officer present during the execution of the warrant must prepare and verify an inventory of any property seized." Fed. R. Crim. P. 41(e)(1) and (f)(1)(B); see 18 U.S.C. 3105; see also, *e.g.*, *Los Angeles Cnty.* v. *Rettele*, 550 U.S. 609, 610 (2007) (per curiam) ("The warrant authorized [the officer] to search the homes and three of the suspects for documents and computer files.").

Section 2703, by contrast, does not expressly authorize law enforcement officers to enter private premises against the wishes of a provider. Instead, the statute provides that the government "may *require the disclosure* by a provider" of certain electronic communications. 18 U.S.C. 2703(a) (emphasis added); see 18 U.S.C. 2703(b)(1) (government "may require a provider * * * to disclose" communications); 18 U.S.C. 2703(c)(1)

(government "may require a provider * * * to disclose" other records). The statute further clarifies that "the presence of an officer shall not be required for service or execution of" a Section 2703 warrant. 18 U.S.C. 2703(g). In other words, a Section 2703 warrant compels a service provider to gather any responsive materials in the provider's control, rather than mandating that a law enforcement officer do so.

The execution of a Section 2703 warrant thus functions like the execution of a subpoena. With a subpoena, a court "may order the witness to produce any books, papers, documents, data, or other objects the subpoena designates." Fed. R. Crim. P. 17(c)(1). It then becomes the witness's responsibility "to produce the designated items." *Ibid.* That is precisely what happened here. Law enforcement did not demand entry into Microsoft's offices to search the facilities and forcibly search for and seize documents or computers; it "served" the Section 2703 warrant "on Microsoft at its headquarters in Redmond, Washington." Pet. App. 2a. In practice, that is how both subpoenas and Section 2703 warrants are served—by transmitting the demand for disclosure to a provider.

Second, in enacting the SCA, Congress was well aware that a Section 2703 warrant would not operate like a traditional search warrant. Congress described a Section 2703 warrant as "a warrant *issued using the procedures* described in the Federal Rules of Criminal Procedure." 18 U.S.C. 2703(a), (b)(1)(A), and (c)(1)(A) (emphasis added). The 2001 amendments to the SCA underscore that Congress did not intend to equate Section 2703 warrants and conventional warrants. Those amendments struck prior language indicating that a warrant must be obtained "under the Federal Rules of

Criminal Procedure" and substituted the language that Section 2703 warrants must be obtained "using the procedures described in the Federal Rules of Criminal Procedure." Patriot Act § 220(a)(1), 115 Stat. 291-292. That change confirms Congress's view that a Section 2703 warrant is not a species of a traditional search warrant but rather a distinct mechanism that employs some of the procedures of Federal Rule of Criminal Procedure 41, though not all of the practices for executing a conventional search warrant.

Other portions of the statute further demonstrate that Congress understood that a Section 2703 warrant would be executed differently. As already mentioned, the SCA provides that no law enforcement officer need be present at the time of execution. 18 U.S.C. 2703(g). It also provides that a broader array of courts may issue warrants, including any court with jurisdiction over the offense being investigated or any court in the district in which a provider is located, rather than just the district in which the property is located. Compare 18 U.S.C. 2711(3)(A), with Fed. R. Crim. P. 41(b)(1). Both distinctions reflect Congress's creation of a new technique for compelling the disclosure of records: a probable-cause-based "warrant" that is executed like a subpoena.

Third, Microsoft's own challenge to the enforcement of the Section 2703 warrant at issue here borrows from challenges to subpoenas rather than challenges to traditional search warrants. Upon being served with the warrant, Microsoft filed what was effectively a motion to quash. Pet. App. 3a; see C.A. App. A20-A34 (Microsoft's "motion to vacate" the warrant) (capitalization

altered; emphasis omitted).[3] After the district court denied its motion, Microsoft refused to produce the requested records, and the district court held it in civil contempt. Pet. App. 3a. A subpoena recipient likewise may file a motion to quash or modify the subpoena, Fed. R. Crim. P. 17(c)(2), and a court may hold a noncomplying subpoena recipient in contempt. Fed. R. Crim. P. 17(g). Meanwhile, parties may not raise such pre-enforcement challenges to traditional search warrants, which are often executed without prior notice. See Fed. R. Crim. P. 41(f)(1)(C) (providing that officer must leave "a copy of the warrant and a receipt for the property taken" after the search). The process of challenging a search warrant is thus retrospective, accomplished through a motion to suppress evidence found in the search. See *United States* v. *Grubbs*, 547 U.S. 90, 99 (2006) ("The Constitution protects property owners not by giving them license to engage the police in a debate over the basis for the warrant, but by interposing, *ex ante*, the deliberate, impartial judgment of a judicial officer * * * and by providing, *ex post*, a right to sup-

---

[3] The SCA authorizes providers to file a motion to quash or modify a 2703(d) order, see 18 U.S.C. 2703(d), but does not establish the same procedure for challenging Section 2703 warrants. Microsoft's motion to quash thus appears to rely on the background principle that such challenges are available to subpoena recipients or other recipients of disclosure orders. See *Donovan*, 464 U.S. at 414-415 (explaining that subpoenas are executed "after adequate opportunity to present objections") (quoting *Oklahoma Press Publ'g Co.* v. *Walling*, 327 U.S. 186, 195 (1946)); see also *City of L.A.* v. *Patel*, 135 S. Ct. 2443, 2453 (2015) (holding that "a hotel owner must be afforded an opportunity to have a neutral decisionmaker review an officer's demand to search the [guest] registry before he or she faces penalties for failing to comply") (emphasis omitted).

press evidence improperly obtained and a cause of action for damages.") (citation and internal quotation marks omitted).

3. Faced with the long history of the enforceability of subpoenas seeking information stored abroad, the court of appeals attempted to distinguish Section 2703 warrants in two ways: It emphasized that warrants and subpoenas are "distinct legal instruments," Pet. App. 31a, and it suggested that there may be a "caretaker" exception to the subpoena rules, *id.* at 34a. Neither distinction has force.

As to the first, it is true that warrants and subpoenas are different instruments. Section 2703's warrant requirement no doubt provides "a greater level of protection to priority stored communications." Pet. App. 31a. But the important question is *how* it achieves that greater protection. As explained above, see pp. 2-4, *supra*, Congress increased privacy protections for what it considered more sensitive information by ratcheting up the governmental showing necessary to acquire the information. Under the SCA's three-tiered hierarchy for disclosure, the government can acquire the most sensitive category of information only by making a showing of probable cause and particularity. See 18 U.S.C. 2703(a), (b)(1)(A), and (c)(1)(A). The level of required suspicion thus drives the "warrant" label. But the level of required suspicion does not alter the statutory reality that the Section 2703 warrant is executed like a subpoena. See pp. 34-39, *supra*.

The SCA nowhere suggests that a Section 2703 warrant protects privacy not just by imposing a probable-cause standard but also by foreclosing access to documents stored abroad. Indeed, that would result in a bizarre bifurcation of the statute: Emails stored for more

than 180 days could be demanded by subpoena with notice, which would not distinguish between emails that a provider stores in the United States and emails that it stores abroad. See 18 U.S.C. 2703(a) and (b)(1)(B)(i). But emails stored for fewer than 181 days could be demanded only by a warrant, which would preclude the disclosure of any emails that the provider stores abroad. See 18 U.S.C. 2703(a). Perhaps even more oddly, if the government were to forgo a subpoena and instead obtain a Section 2703 warrant—under the *higher* showing of probable cause—it would lose its ability to demand certain foreign-stored emails. Put differently, under the court of appeals' theory of the SCA, law enforcement would have more limited access to records sought through a warrant than through a subpoena. The court gave no reason why Congress might have embedded that distinction into a statute that purports to give the government three alternative mechanisms to obtain electronic communications.

The court of appeals separately suggested that subpoenas might not cover circumstances in which the government seeks "to compel a recipient to produce an item under its control and located overseas when the recipient is merely a caretaker for another individual or entity and that individual, not the subpoena recipient, has a protectable privacy interest in the item." Pet. App. 34a. But the panel did not cite any support for such a "caretaker" exception. Because the production of documents has traditionally turned on control rather than ownership, courts have enforced subpoenas against parties who hold documents on others' behalf. See, *e.g.*, *In re Grand Jury Subpoena Served Upon Horowitz*, 482 F.2d 72 (2d Cir.) (Friendly, J.) (partially enforcing subpoena requiring an accountant to produce the contents

of locked filing cabinets that belonged to a client but to which the accountant had access), cert. denied, 414 U.S. 867 (1973); *United States* v. *Barr*, 605 F. Supp. 114 (S.D.N.Y. 1985) (upholding subpoena requiring mail delivery service to turn over a client's letters); see also *Fisher* v. *United States*, 425 U.S. 391 (1976) (rejecting Fifth Amendment challenge to subpoena directed at taxpayers' attorneys).

Moreover, the fact that a user may have a separate privacy interest in the contents of his or her emails is beside the point here. In this case, the government obtained a probable-cause-based warrant, which, as discussed, is the traditional mechanism for protecting individuals' privacy. See p. 28, *supra*. That is presumably why Microsoft does not dispute that it must disclose the contents of any emails stored in the United States, even though it is just as much a "caretaker" here as abroad. See Pet. App. 10a. The Second Circuit's proposed exception therefore does not reflect any heightened privacy interest in the contents of emails stored by a provider. Instead, it gives additional protection to the contents of foreign-stored emails, even though Microsoft chooses where to store emails without the user's knowledge or consent. The common-law principles governing subpoenas do not recognize any such distinction.

C. Microsoft's Contrary Theory Would Be Both Impractical And Detrimental To Law Enforcement

Microsoft's theory of the SCA, which depends on where data is stored, would create serious administrability concerns and would hamper domestic law enforcement and counterterrorism efforts. Those real-world consequences further suggest that Congress did not adopt the scheme that Microsoft proposes. See *Maracich* v. *Spears*, 133 S. Ct. 2191, 2203 (2013) (explaining

that statutes should be interpreted in light of their object and policy); cf. *RJR Nabisco*, 136 S. Ct. at 2105 (noting that the "troubling consequences" of restricting RICO to domestic enterprises "reinforce[d]" the Court's "conclusion, based on [the statute's] text and context").

1. Under Microsoft's theory, the location of the requested data would determine whether a provider must comply with Section 2703. But where that data is located depends solely on a provider's business decision, made without a user's knowledge or consent and subject to change at any moment. A provider's choice where to store its data may not bear any relationship to the user's ties to the United States. Under Microsoft's theory, a U.S. provider doing business in the United States need not disclose an email about a crime in the United States, even though that email can be retrieved by the U.S. provider at its U.S. offices. That remains true even if the user who sends the email is a U.S. citizen living in the United States, communicating with another U.S. citizen living in the United States. On this record, so long as the user stated upon creation of his email account that he is "from" a foreign country, his emails will be stored in or near that country and will be off-limits to U.S. law enforcement under a Section 2703 warrant. J.A. 30-31; see, *e.g.*, Vermont Cert. Amicus Br. 7 (describing data requests involving suspects who live in Vermont). Such a policy, combined with the Second Circuit's decision, creates "a roadmap for even an unsophisticated person to use email to facilitate criminal activity while avoiding detection by law enforcement." Pet. App. 126a (Cabranes, J., dissenting).

What is more, the same result would hold even if Microsoft chose to move *all* of its servers outside the

United States. If, at its sole discretion, it decided to store all emails sent by U.S. subscribers on servers located in Canada or Mexico, all emails would fall outside the purview of the SCA. Congress did not enact a disclosure scheme that a U.S. provider could nullify by the expedient of shifting data to storage devices that it locates over the border. To allow that result would permit a private provider in the United States to thwart Section 2703's critical role in assisting law enforcement to combat terrorism and crime.

2. Microsoft's data-location theory produces equally harmful results when applied to other service providers that have different corporate systems for storing data. Microsoft, at least, currently stores emails for a single account in a particular location that it can divine through a few keystrokes. See J.A. 34. Google, by contrast, stores the emails of U.S. users all over the world, sometimes breaking an account into multiple "shards"; even a single email may be divided into pieces, with the text stored in one location and attachments in another. See Pet. App. 127a-128a (Cabranes, J., dissenting); see also *In re the Search of Content That Is Stored at Premises Controlled by Google*, No. 16-mc-80263, 2017 WL 1487625, at *1 (N.D. Cal. Apr. 25, 2017) ("User files may be broken into component parts, and different parts of a single file may be stored in different locations (including different countries)."). Because it also moves the location of the data frequently and without human intervention, Google's compliance with a Section 2703 warrant would depend on the happenstance of where the data is located at the precise moment when the warrant is served or the provider accesses its network. See *In re Search of Information Associated with [Re-*

dacted]@gmail.com That Is Stored at Premises Controlled by Google, Inc., No. 16-mj-757, 2017 WL 3445634, at *2 (D.D.C. July 31, 2017) (*In re Premises Controlled by Google*). And that is assuming that the precise location is knowable; some providers may not even be able to determine whether they currently store the requested data in the United States or abroad. See Pet. App. 128a (Cabranes, J., dissenting).

3. Without the Section 2703 warrant process, the government lacks an equally effective means of accessing electronic data critical to law enforcement and national security. Extrajudicial processes cannot provide a reliable substitute to reach data stored abroad. Microsoft has argued, and the court of appeals observed, see Pet. App. 45a-47a, that the government may ask foreign law enforcement to gather and share certain foreign-stored data under a mutual legal assistance treaty (MLAT). But for several reasons, MLATs are often not an effective alternative to requiring disclosure of emails under the SCA.

First, MLATs are not universal: The government has entered into bilateral MLATs with fewer than half of the world's nations. See Statement of Brad Wiegmann, Deputy Assistant Att'y Gen., DOJ, Before the Subcomm. on Crime & Terrorism, U.S. Senate Comm. on the Judiciary, Hearing entitled: *Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights* 6 (May 24, 2017), https://www.judiciary.senate.gov/imo/media/doc/05-24-17%20Wiegmann%20Testimony.pdf (Wiegmann Statement).

Second, to the extent that an MLAT covers the requested data in a particular case, the process can be slow and uncertain, often taking many months or even

years to generate results. See Wiegmann Statement 6, 9; Pet. App. 90a; see also, *e.g.*, *In re Grand Jury Subpoenas Dated March 19, 2002 and August 2, 2002*, 318 F.3d 379, 381-382 (2d Cir. 2003) (describing MLAT request for bank records held in a foreign country that had not been completed after more than two years). A foreign government may also retain discretion under an MLAT to deny assistance in certain circumstances. See Pet. App. 90a-91a.

Third, with respect to providers such as Google, resorting to the MLAT process would be futile. Because Google constantly moves data around the world, the location of the data at any given moment in time is difficult or impossible to ascertain—a problem compounded by splitting a single email into separate pieces of data. See, *e.g.*, *In re Search Warrant No. 16-960-M-01 to Google*, 232 F. Supp. 3d 708, 725 (E.D. Pa. 2017) ("[I]t would be impossible for the Government to obtain the sought-after user data through existing MLAT channels."). As one district court explained, "[b]y the time the MLAT process had begun, any electronic communications targeted in an SCA warrant could have moved to a completely different country, making the effort to obtain this evidence a global game of whack-a-mole." *In re Premises Controlled by Google*, 2017 WL 3445634, at *26. On top of that, even if the location of the data could be identified at the critical moment, some U.S. providers permit only U.S. personnel to access it. *Ibid.* Thus, under the Second Circuit's decision, data that providers such as Google store abroad would effectively remain beyond the reach not only of the MLAT process but also of both U.S. and foreign law enforcement.

D. Enforcement Of Section 2703 Respects The United States' International Obligations

Courts developed the presumption against extraterritoriality in part "to protect against unintended clashes between our laws and those of other nations which could result in international discord." *Kiobel* v. *Royal Dutch Petroleum Co.*, 569 U.S. 108, 115 (2013) (quoting *EEOC* v. *Arabian Am. Oil Co.*, 499 U.S. 244, 248 (1991)). Pointing to that motivating principle, Microsoft contends that Section 2703's application to foreign-stored data threatens international discord and "place[s] U.S. companies in the untenable position of being forced to violate foreign privacy laws to comply with U.S. warrants." Br. in Opp. 25. Those results have not materialized in any significant way. To the contrary, the United States' position in this case is consistent with many other countries' practices and with U.S. treaty obligations.

1. Microsoft worries that the enforcement of Section 2703 in this case will launch a "global free-for-all." Br. in Opp. 5. Experience refutes that claim. As an initial matter, a disclosure-focused construction of Section 2703 already applies in every court to have issued a written opinion on the matter outside of the Second Circuit, see p. 21 n.2, *supra*, and no such negative consequences have ensued. Moreover, construing Section 2703 to cover foreign-stored data comports with the approach of many other nations. See Wiegmann Statement 6 (observing that "other countries do not restrict their own ability to demand data stored outside their borders"); see also *id.* at 12 (listing examples). One comparative study of the United States, Australia, Canada, Japan, and six European countries concluded that only two, "in some instances, limit the data that the government can access to that which is physically located

on servers within their national borders." Winston Maxwell & Christopher Wolf, *A Global Reality: Governmental Access to Data in the Cloud* 2 (July 18, 2012), https://www.hldataprotection.com/uploads/file/Revised%20Government%20Access%20to%20Cloud%20Data%20Paper%20(18%20July%2012).pdf. In the other countries, the government may require a "service provider to disclose customer data in certain situations, and in most instances this authority enables the government to access data physically stored outside the country's borders, provided there is some jurisdictional hook, such as the presence of a business within the country's borders." *Id.* at 2-3 (emphasis omitted).

This case illustrates the imbalance that Microsoft's theory would create. The requested data is stored in Ireland. See Pet. App. 7a, 10a. In the Second Circuit, Ireland filed a brief as amicus curiae, explaining that "there may be circumstances in which an Irish court would order the production of records from an Irish entity on foreign soil." Ireland C.A. Amicus Br. 6; see *id.* at 7 ("[O]n the central point whether it had power to order production of documents by an Irish registered company by one of its branches situated in a foreign country, the [Irish] Supreme Court found that it did."). The brief further noted that an Irish court would exercise that authority, however, "only after being competently apprised of whether the execution of the order would violate the law of the foreign sovereign" and only after "certain matters are demonstrated." *Id.* at 6-7. But whatever restrictions it imposes, Ireland possesses the raw power that Microsoft asks this Court to deem surrendered by Congress.

2. Microsoft's restrictive reading of the SCA would also undermine the United States' compliance with its

treaty obligations. The United States is one of 55 parties to the Council of Europe Convention on Cybercrime, Nov. 23, 2001, S. Treaty Doc. No. 11, 108th Cong., 1st Sess. (2003) (Treaty Doc. 11), 2296 U.N.T.S. 167, often called the Budapest Convention. The Budapest Convention is designed to address cybercrime, including "the risk that computer networks and electronic information may * * * be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks." Convention on Cybercrime, Preamble. Among other things, it requires parties to "adopt such legislative and other measures as may be necessary to empower its competent authorities to order" any "person in its territory to submit specified computer data in that person's possession or control." *Id.* art. 18.1(a).

Article 18.1(a) covers the power at issue in this case. In the ratification process, the Department of State explained that the term "person" includes a "third party custodian of data, such as an [Internet service provider]." Letter of Submittal, Treaty Doc. 11, at XV (Sept. 11, 2003); see Convention on Cybercrime, Explanatory Report ¶ 26 (Nov. 8, 2001) (describing a "service provider" as a "category of persons"); Cybercrime Convention Committee, Council of Europe, *T-CY Guidance Note #10*, at 6 (Mar. 1, 2017) (Convention Guidance Note 10) (providing non-binding guidance that the term "person" includes a "service provider"), https://www/coe.int/en/web/cybercrime/guidance-notes. And the Explanatory Report adopted by the Convention's negotiators and submitted to the Senate with the treaty further clarified that the term "possession or control" includes "situations in which the data to be produced is

outside of the person's physical possession but the person can nonetheless freely control production of the data from within the ordering Party's territory." Convention on Cybercrime, Explanatory Report ¶ 173; see Convention Guidance Note 10, at 6. Putting all of that together, Article 18.1(a) requires the United States to ensure that its relevant authorities have the power to compel the production of data within a domestic service provider's possession or control. See Convention Guidance Note 10, at 7 ("The storage of subscriber information in another jurisdiction does not prevent the application of Article 18 Budapest Convention as long as such data is in the possession or control of the service provider.").

Section 2703 of the SCA enables the United States to fulfill that obligation. Because Section 2703 already provided law enforcement personnel with the necessary authority to demand disclosure from U.S. service providers, Congress did not pass implementing legislation when the Senate ratified the Budapest Convention in 2006. See Letter of Transmittal, Treaty Doc. 11, at III (Nov. 17, 2003) (noting, after reservations and declarations irrelevant here, that "the Convention would not require implementing legislation for the United States"); *id.* at VI ("The Convention would not require implementing legislation for the United States."); S. Exec. Rep. No. 6, 109th Cong., 1st Sess. 3 (2005) (explaining that the "investigative tools" required by Articles 16 through 21 "are already provided for under U.S. domestic law"). Adoption of Microsoft's restrictive view of the SCA would thus undermine the United States' compliance with its obligations under Article 18 of the Budapest Convention.

3. Nevertheless, Microsoft asserts that its data-location theory is necessary to protect U.S. service providers from conflicting obligations at home and abroad. That fear is speculative. In the course of this litigation, Microsoft has never stated that it would be subject to liability under the laws of Ireland or the European Union for disclosing in the United States any communications stored at its Dublin datacenter. See J.A. 140, 149. Nor did Ireland expressly assert such a conflict in its brief as amicus curiae, though it hinted that Irish data protection laws might apply. See Ireland C.A. Amicus Br. 3-7. In fact, Microsoft has not identified a single example of a U.S. service provider that has been compelled to disclose foreign-stored data under Section 2703 and has been sanctioned by a foreign nation for doing so. That is so even though Microsoft complied with Section 2703 warrants until this litigation commenced, see J.A. 30 (noting that the Dublin datacenter has been operational since 2010), and even though Section 2703 warrants have continued to be enforced outside the Second Circuit since the decision below, see p. 21 n.2, *supra*.

In any event, if an actual conflict of laws were to arise, our judicial system is equipped to handle that scenario. The government could exercise discretion to pursue alternate channels, where available. See Wiegmann Statement 11 (noting that the government "typically" resolves such situations "through closer inquiry or good-faith negotiation"); J.A. 117 (discussing close cooperation between the United States and "Western European law enforcement officials"). It could also modify the request, or drop it altogether. See Wiegmann Statement 11.

When the government chooses instead to pursue enforcement of a Section 2703 warrant, "[i]t is well settled

that [foreign statutes] do not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that statute." *Société Nationale Industrielle Aérospatiale*, 482 U.S. at 544 n.29; see *In re Sealed Case*, 832 F.2d at 1283 ("[T]here is little doubt that a United States Court has the power to order any party within its jurisdiction to testify or produce documents regardless of a foreign sovereign's views to the contrary.") (brackets, citation, and internal quotation marks omitted). In some circumstances, however, courts have accounted for competing foreign laws when a party refuses to comply with a U.S. disclosure order, often by consulting Section 442 of the Restatement (Third) of the Foreign Relations Law of the United States (1987) (Restatement (Third)). See, *e.g.*, *Société Nationale Industrielle Aérospatiale*, 482 U.S. at 544 n.29;[4] *Linde* v. *Arab Bank, PLC*, 706 F.3d 92, 109-110 (2d Cir. 2013), cert. denied, 134 S. Ct. 2869 (2014); *Reinsurance Co. of Am., Inc.* v. *Administratia Asigurarilor de Stat*, 902 F.2d 1275, 1281-1282 (7th Cir. 1990).

Section 442 of the Restatement (Third) provides that a U.S. court may require the recipient of a disclosure order "to make a good faith effort to secure permission from the foreign authorities to make the information available," and cautions that a court should hesitate to impose harsh sanctions if the recipient's good-faith efforts abroad prove unsuccessful. Restatement (Third)

---

[4] *Société Nationale Industrielle Aérospatiale* referred to Section 437(1)(c) of a tentative draft of the Restatement (Third), but that section ultimately became Section 442 in the final version of the Restatement (Third). See 482 U.S. 544 n.28.

§ 442(2).[5] Although sanctions may be appropriate even when the party's non-production is the result of its compliance with foreign law, the party's "inability to comply [with a production order] because of foreign law" can be a "weighty excuse for nonproduction." *Societe Internationale pour Participations Industrielles et Commerciales, S. A.* v. *Rogers*, 357 U.S. 197, 211-212 (1958). Courts' tendency, at least at the contempt stage, to weigh a party's competing foreign obligations mitigates any unfairness to regulated entities such as Microsoft, if a square conflict between U.S. law and foreign law were to materialize. And more to the point, the possibility of a future conflict between U.S. and foreign law does not change the best construction of an important domestic law enforcement and counterterrorism tool enacted more than 30 years ago.

---

[5] The American Law Institute has approved Section 306 of the Restatement (Fourth) of the Foreign Relations Law of the United States (2016) (Restatement (Fourth)), which replaces Section 442 of the Restatement (Third). See ALI, *The Foreign Relations Law of the United States, Status Details*, https://www.ali.org/projects/show/foreign-relations-law-united-states/; Restatement (Fourth) § 306 Reporters' Note 8. Section 306 states that a U.S. court "may impose sanctions on a person who fails to comply with an order to produce evidence • • • even if complying with the order would subject the person to punishment under foreign law." Restatement (Fourth) § 306(2). Where permissible, though, the court may "take[] into account the significance of the evidence sought to the underlying proceeding, the good-faith efforts of the person to comply with the order in light of obstacles imposed by foreign law, and the legitimate interests of the foreign sovereign with respect to its law" when "deciding what sanctions to apply to enforce its order." *Ibid.*

CONCLUSION

The judgment of the court of appeals should be reversed.

Respectfully submitted.

NOEL J. FRANCISCO
Solicitor General
JOHN P. CRONAN
Acting Assistant Attorney General
MICHAEL R. DREEBEN
Deputy Solicitor General
MORGAN L. GOODSPEED
Assistant to the Solicitor General
ROSS B. GOLDMAN
Attorney

DECEMBER 2017

APPENDIX

1. 18 U.S.C. 2701 provides:

Unlawful access to stored communications

(a) OFFENSE.—Except as provided in subsection (c) of this section whoever—

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

(b) PUNISHMENT.—The punishment for an offense under subsection (a) of this section is—

(1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State—

(A) a fine under this title or imprisonment for not more than 5 years, or both, in the case of a first offense under this subparagraph; and

(B) a fine under this title or imprisonment for not more than 10 years, or both, for any subsequent offense under this subparagraph; and

(2) in any other case—

(A) a fine under this title or imprisonment for not more than 1 year or both, in the case of a first offense under this paragraph; and

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under this subparagraph that occurs after a conviction of another offense under this section.

(c) EXCEPTIONS.—Subsection (a) of this section does not apply with respect to conduct authorized—

(1) by the person or entity providing a wire or electronic communications service;

(2) by a user of that service with respect to a communication of or intended for that user; or

(3) in section 2703, 2704 or 2518 of this title.

2. 18 U.S.C. 2702 (2012 & Supp. IV 2016) provides:

Voluntary disclosure of customer communications or records

(a) PROHIBITIONS.—Except as provided in subsection (b) or (c)—

(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and

(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

(b) EXCEPTIONS FOR DISCLOSURE OF COMMUNICATIONS. —A provider described in subsection (a) may divulge the contents of a communication—

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

(2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;

(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A;

(7) to a law enforcement agency—

(A) if the contents—

(i) were inadvertently obtained by the service provider; and

(ii) appear to pertain to the commission of a crime; or

[(B) Repealed. Pub. L. 108-21, title V, § 508(b)(1)(A), Apr. 30, 2003, 117 Stat. 684]

(8) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.

(c) EXCEPTIONS FOR DISCLOSURE OF CUSTOMER RECORDS.—A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))—

(1) as otherwise authorized in section 2703;

(2) with the lawful consent of the customer or subscriber;

(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(4) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency;

(5) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A; or

(6) to any person other than a governmental entity.

(d) REPORTING OF EMERGENCY DISCLOSURES.—On an annual basis, the Attorney General shall submit to the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate a report containing—

(1) the number of accounts from which the Department of Justice has received voluntary disclosures under subsection (b)(8);

(2) a summary of the basis for disclosure in those instances where—

(A) voluntary disclosures under subsection (b)(8) were made to the Department of Justice; and

(B) the investigation pertaining to those disclosures was closed without the filing of criminal charges; and

(3) the number of accounts from which the Department of Justice has received voluntary disclosures under subsection (c)(4).

3. 18 U.S.C. 2703 provides:

Required disclosure of customer communications or records

(a) CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN ELECTRONIC STORAGE.—A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. A governmental

entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN A REMOTE COMPUTING SERVICE.—(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(c) RECORDS CONCERNING ELECTRONIC COMMUNICATION SERVICE OR REMOTE COMPUTING SERVICE.—(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction;

(B) obtains a court order for such disclosure under subsection (d) of this section;

(C) has the consent of the subscriber or customer to such disclosure;

(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the—

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal

or State grand jury or trial subpoena or any means available under paragraph (1).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

(d) REQUIREMENTS FOR COURT ORDER.—A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(e) NO CAUSE OF ACTION AGAINST A PROVIDER DISCLOSING INFORMATION UNDER THIS CHAPTER.—No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.

(f) REQUIREMENT TO PRESERVE EVIDENCE.—

(1) IN GENERAL.—A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) PERIOD OF RETENTION.—Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

(g) PRESENCE OF OFFICER NOT REQUIRED.—Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

4. 18 U.S.C. 2711 provides:

Definitions for chapter

As used in this chapter—

(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section;

(2) the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system;

(3) the term "court of competent jurisdiction" includes—

(A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that—

(i) has jurisdiction over the offense being investigated;

(ii) is in or for a district in which the provider of a wire or electronic communication service is located or in which the wire or electronic communications, records, or other information are stored; or

(iii) is acting on a request for foreign assistance pursuant to section 3512 of this title; or

(B) a court of general criminal jurisdiction of a State authorized by the law of that State to issue search warrants; and

(4) the term "governmental entity" means a department or agency of the United States or any State or political subdivision thereof.